Description of Actual State Sensor Types for the Configuration Management (CSM) Capability

7 Jul 2014

1 Purpose

This document is intended to provide insight on the types of tools and technologies that can be utilized to support the collection of security-related configuration settings required to perform the CSM capability as part of Continuous Diagnostics and Mitigation (CDM). The 'Description of Generic Sensor Types for the Continuous Diagnostic and Mitigation (CDM) Collection System' document described the Actual State sensor types for CDM including potential operational impacts and general data accuracy issues associated for each sensor type.

The CSM capability provides an organization visibility into risks associated with improper or non-compliant security-related configuration settings for authorized hardware and software. When available, the CSM capability provides a method to ensure software security-related configuration settings conform to the Common Configuration Enumeration (CCEs) configuration guidance statements. This capability is dependent on the existence of both an authorized hardware and authorized software inventory as developed by the Hardware and Software Asset Management capabilities.

The CSM capability relies on many different sensors on the network to collect security-related configuration settings. These sensors directly and indirectly collect configuration settings information from each device connected to the network. The following are examples of how common tools and technologies can be employed as Actual State sensors to support the CSM capability.

2 CSM Actual State Sensor Types

2.1 Active Network Sensor

An Active Network Sensor actively probes the network or devices over the network.

To support CSM, an Active Network Sensor probes or queries assets (both hardware and software) to determine security-related configuration settings currently implemented. These checks are done periodically by either authenticating directly with the device or querying the device in a non-authenticated manner. Individually enumerating each device may not be practical for large enterprises. Depending on the network size, employing Active Network Scanners to collect every security-related configuration setting can be both resource and time intensive; organizations should consider this before employing this type of Actual State sensor.

Active Network Sensor examples include the United States Government Configuration Baseline (USGCB) scanners, authenticated vulnerability scanners, authenticated configuration scanners, or any software/application scanner that can support configuration control/management of security-related configuration settings.

USGCB scanners audit and assess a device to determine its compliance using National Institute of Standards and Technology (NIST) USGCB content. USGCB content consists of security configuration baselines for IT products widely deployed across the federal agencies. USGCB scanners scan devices to assess whether the installed software or applications are compliant with applicable security configuration guides.

In support of the CSM capability, some authenticated vulnerability scanners scan devices to determine if a device is vulnerable to exploitation due to an insecure configuration setting.

Authenticated configuration scanners audit and assess a device using the device's system logon privileges to determine the device's compliance with a defined set of configuration requirements (i.e., applicable security configuration guides). By using a device's system logon privileges, authenticated configuration scanners can provide more accurate configuration setting information. In contrast, non-credentialed configuration scanners are not as effective in collecting configuration settings due to lack of direct non-privileged system access.

2.2 Passive Network Sensor

A Passive Network Sensor is designed to capture and/or collect network traffic that passes across a monitored network link.

A Passive Network Sensor only collects data as it traverses the network segment it is configured to monitor; therefore, only data from devices that are communicating on the monitored network segment will be collected. This allows for both precise but limited monitoring of devices depending on the configuration scope of the Passive Network Sensor. However, in regards to supporting the CSM capability, Passive Network Sensors are mostly limited to collecting accurate security-related configuration setting information related to enabled protocols and services. Some other types of configuration setting data may be inferred based on how a device is communicating but usually this data would need to be substantiated with other more authoritative Actual State sensors. Similar to non-credentialed configuration scanners described above, information collected from Passive Network Sensors is often not specific enough due to being collected without direct privileged access to the device.

Passive Network Sensor examples include packet and protocol analyzers. These analyzers can detect a device communicating on a network using a port, protocol, or service that is supposed to be removed/blocked based on configuration settings policy.

2.3 Asset Management Repository

An Asset Management Repository is a collection of data created and updated as part of a process or activity that manages that asset for an organization.

Many Asset Management Repositories aggregate security-related configuration data that is collected on in-scope devices from various tools and processes deployed to manage these devices for a purpose other than CDM. Asset Management Repositories should be used as data sources for the CSM capability whenever possible because they can provide the data without needing to deploy additional sensors on the network. Examples include mobile device management (MDM) suites, policy audit tools, or other asset management tools that collect or store configuration setting data.

Traditional scanners and host-based agents are not designed to work with mobile devices, so MDM suites are used for identifying, maintaining, and updating information about device state and health (e.g., device settings). The data collected by these managers can be utilized to provide security-related configuration settings of each managed mobile device to CDM.

The Network Configuration Protocol (NETCONF) is used for managing and retrieving posture attribute data from network infrastructure endpoints. Instead of scanning or installing endpoint-based agents on these devices, an organization can use the data collected via NETCONF and used by their existing infrastructure endpoint management software.

Enterprise management tools that use Simple Network Protocol (SNMP) for managing and retrieving posture attribute data from endpoints on a network can provide information for CSM.

Audit management systems that collect audit logs from devices can support CSM if they collect events related to changes of security-related configuration settings.

Another example is Microsoft's Group Policy feature. Microsoft defines Group Policy as a feature that provides an infrastructure for centralized configuration management of the operating system and applications that run on the operating system. Group Policies can be used to enforce specific configuration settings on devices. Group Policy information, as well as other security-related configuration setting information, is stored within Active Directory.

2.4 Network Event Sensor

A Network Event Sensor is designed to detect and report events of interest to a defined location in a timely manner.

Network event sensors provide situational awareness of unauthorized events that take place on the network. These sensors perform this by monitoring and alerting on predefined audit security and compliance relevant information received from in-scope devices. Managed devices on the network forward audit log data via specified management protocols to a Network Event Sensor. What events and when to report is defined by the parameters of the security policy that are in-turn applied to each in-scope device. Once the Network Event Sensor receives events, the events can be analyzed through real-time data correlation and analysis of historical trends to track security-related configuration settings.

Examples of common tools employed to support the CSM capability include security information and event management (SIEM) tools and event log analyzers. SIEM software aggregate logs relevant to security-related configuration settings from in-scope devices. SIEM enable policies to be configured on the network to alert when a configuration change has occurred on a network device. An alert will be sent to the SIEM if an unauthorized configuration change occurs or is attempted. The SIEM can correlate and analyze alert data for all in-scope devices.

SIEM, intrusion detection systems (IDS), and intrusion prevention systems (IPS) tools can identify active/enabled ports, protocols, or services that are supposed to be uninstalled or disabled according to configuration setting policies.

Network Event Sensors require careful management to avoid information overload as a result of improperly configured event thresholds and triggers. Too many alerts could result in the inability to accurately detect configuration setting information.

2.5 Endpoint-Based Agent

An Endpoint-Based Sensor is a software client installed on, or natively embedded within, the operating system of a device.

Endpoint-Based Agents collect and report security-related configuration settings on software products installed on in-scope devices. This method of collecting security-related configuration settings is the most direct and accurate; however, it requires an installed agent for every managed device resulting in an increase in management overhead.

Endpoint-based agents provide some of the most accurate CSM data due to the direct relationship with the device and its associated software products. Examples include configuration management agents, endpoint management and security agents, and built-in OS functionality. Each of these agents monitor, detect, and report current, to include changes to, security-related configuration settings. Reporting is accomplished by pushing security-related configuration information to a centralized management server or by storing and waiting until an agent controller request or retrieves the information. Reporting can be immediate or periodically based upon a predetermined frequency.

Supporting the CSM capability, native OS functionality acting as an Endpoint-Based Sensor can provide near real time detection and reporting of current security-related configuration settings. For example, organizations can use TNC endpoint technology to ensure devices comply with enterprise security policies. TNC provides the standards-based mechanisms to support the secure exchange of security-related configuration information. This information exchange can occur on demand, at a preset periodicity, or based on an event (e.g., connection of the device to the network, when a setting is changed).